AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with Telephone Number (276) 608-7196 that is stored at premises controlled by Verizon

Case No. 1:21mj105

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of New Jersey , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1951	Conspiracy to Interfere with Commerce by Threats or Violence (Hobbs Act robbery)

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Peter Gonzalves, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/28/21

Judge's signature

City and state: Abingdon, VA

Honorable Pamela Meade Sargent, USMJ
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ABINGDON DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH (276) 608-7196 THAT IS STORED AT PREMISES CONTROLLED BY VERIZON	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Peter Gonzalves, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Verizon, a wireless provider whose Subpoena Compliance Department is headquartered at 180 Washington Valley Rd, Bedminster NJ 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Verizon to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am an investigative law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 United States Code, and am empowered by law to conduct investigations and to make arrests for the offenses enumerated in Section 2516 of Title 18 United States Code.

3. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been so employed since August 2016. I am currently assigned to the Bristol, Virginia Field Office. Prior to becoming an ATF Special Agent, I was a Special Agent with the U.S. Department of State, Diplomatic Security Service for approximately six years. I have taken part in numerous federal, state, and local investigations concerning document and identity fraud, financial fraud, cybercrimes, and firearms and narcotics violations.

4. During my tenure in law enforcement, I have become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds and the organization of drug conspiracies, and methods and techniques commonly employed during the commission of violent crimes, including robbery. In the course of conducting these investigations, I have been involved in the use of the following investigative techniques: interviewing confidential sources and cooperating witnesses; conducting physical surveillance: controlled buys; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen-register data; requesting, collecting and

analyzing billing records; and conducting court-authorized electronic surveillance. Further, I have participated in the preparation, presentation, and execution of numerous search and arrest warrants which have resulted in the recovery of weapons, narcotics, money, and documentary evidence indicative of firearm and narcotic trafficking organizations. Additionally, I have assisted in investigations and arrests leading to convictions for violations of federal and state firearms and narcotics laws to include violent crime.

5. Through instruction and participation in investigations, I have become familiar with the manner and methods by which narcotics traffickers and perpetrators of violent crimes conduct their illegal business and the language and terms that are used to disguise conversations about their illegal activities. From experience and training, I have learned, among other things, that in conversations narcotics traffickers and violent criminals believe susceptible to interception, they virtually never expressly refer to the illegal drugs or weapons or crimes by name; instead to conceal the true nature of their illegal activities and to thwart detection by law enforcement, they refer to the drugs, drug quantities, crimes, and weapons using seemingly innocent terms. I am also aware that violent crime conspiracies are often hatched in advance of the event, and often involve electronic communications between coconspirators and others before and after the crime is perpetrated. These communications often show planning and post-crime

discussions.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1951, Conspiracy to Interfere with Commerce by Threats or Violence (Hobbs Act robbery) have been committed by Michael MILLER and others. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

PROBABLE CAUSE

8. On May 9, 2021, at approximately 8:15 PM, an individual entered Bare's Discount Tobacco and Wine ("Bare's") located at 970 E. Main St. in Abingdon, Virginia, which is located in Washington County in the Western Judicial District of Virginia. According to the store clerk (hereafter known as "Victim 1") who was on duty at the business at the time, the individual produced a handgun and demanded access to the cash register and money safes. Victim 1 described the suspect as a tall and muscular white male, wearing a knit hat, a bandana covering his face, blue jeans, and a green jacket. The clerk also reported the suspect placed a

black handgun on the counter as he demanded cash. At approximately 8:23 PM, the suspect exited the store after taking approximately $35 in cash and two cartons of cigarettes without paying. Other than Victim 1 and the suspect, no additional individuals can be seen on security footage in the store during the time the suspect was inside the business.

9. Bare's sells alcohol, tobacco and packaged food products, many of which were manufactured and/or procured from sources outside the state of Virginia and therefore moved in interstate commerce.

10. Investigators with the Abingdon, Virginia Police Department (APD) later reviewed surveillance footage provided by Bare's and other businesses in the surrounding area. Surveillance footage shows that, at approximately 7:30 PM on May 9 (surveillance footage timestamp), a white Dodge Journey with an unknown license plate (hereafter referred to as "the suspect vehicle") drove around the exterior of Bare's and the adjacent businesses. The suspect vehicle also drove in circles through the parking lots of other businesses in the immediate vicinity.

11. From approximately 8:07 PM through 8:12 PM, the suspect vehicle drove through parking lots of businesses between the BP station located at 906 E. Main St. in Abingdon, Virginia and Bare's. At approximately 8:20 PM, the suspect vehicle can be seen pulling into the BP gas station parking lot. An employee at the BP reported seeing a white Dodge Journey in the parking lot occupied by two

individuals, and that one of the individuals exited the vehicle behind the BP station. At approximately 8:20 PM, an individual wearing similar clothing and matching the physical description of the suspect can be seen walking from the rear of the BP parking lot in the direction of Bare's. At approximately 8:15 PM, the suspect entered Bare's and encountered Victim 1. At approximately 8:23 PM, the suspect exited the store and can be seen on surveillance footage walking from the area of Bare's toward the BP station.

12. On or about May 11, 2021, a Washington County Sheriff's Office (WCSO) investigator reported having a phone conversation with Michael MILLER after the robbery occurred. During this conversation, MILLER informed the investigator he was driving a white Dodge Journey belonging to "B.H." during the previous weekend. B.H. is an associate of MILLER's, though there is no evidence to date of B.H. participating in the conspiracy. The WCSO investigator provided two telephone numbers from which WCSO has received calls from MILLER in weeks and months prior to the robbery: 276-608-7196 and 540-835-3859.

13. On or about May 23, 2021, Verizon produced certain subscriber and device information associated with these two phone numbers. The International Mobile Equipment Identifier (IMEI) associated with 276-608-7196 from March 15, 2021, through May 20, 2021, is 352082504971013. The IMEI associated with 540-835-3859 from April 30, 2021, through May 20, 2021 is 357754083696972. An

IMEI is akin to a unique electronic serial number and identifies a particular device on a cellular network. Verizon's records also indicated the device model associated with 276-608-7196 is a Samsung SM-S111DL. Publicly available information on the internet indicates this device runs Android as its operating system, which is produced and supported by Google.

14. On June 30, 2021, deputies with the WCSO arrested MILLER on outstanding state arrest warrants from other jurisdictions. During a post-*Miranda* interview, MILLER stated he and Robert DAWSON were together in B.H.'s vehicle on the day of the robbery. MILLER stated that, while driving around, DAWSON asked MILLER to drop him off at the BP gas station for an unknown reason. MILLER later stated he and DAWSON discussed how easy it would be to rob Bare's, but MILLER indicated the conversation between him and DAWSON was meant in jest and that he did not actually intend to rob the store. MILLER further stated this conversation took place at Bare's in the afternoon on the day of the robbery, and DAWSON and Victim 1 were both present. MILLER also stated to investigators that Victim 1 is a "dear friend."

15. On June 30, 2021, investigators interviewed Victim 1. Victim 1 stated he/she observed a tall, muscular individual enter the store. After picking up a drink from the cooler, the individual approached the counter, demanded money from the register, and placed a small handgun on the counter. Victim 1 was unable to

determine if it was a real firearm, but described it as small, black, and "old" looking. Victim 1 stated that he/she debated with the individual for several minutes and did not want to open the register for the suspect. Victim 1 stepped out from behind the counter, and the suspect attempted to open the cash register unsuccessfully. The suspect then took approximately $35 in cash from a lockbox and two cartons of cigarettes, both of which were located behind the counter, before leaving the store.

16. Victim 1 also admitted to having a relationship with MILLER. Victim 1 stated that he/she was initially hesitant to disclose that fact as Victim 1 is presently married. Victim 1 further stated that he/she was with MILLER at B.H.'s residence the day after the robbery. Victim 1 also stated the other individual who was with MILLER and Victim 1 at Bare's the day of the robbery was also present. Based on MILLER's and Victim 1's statements, investigators concluded the second male present at B.H.'s residence at that time was DAWSON. That evening, Victim 1 overheard MILLER and DAWSON talking about the robbery. According to Victim 1, MILLER and DAWSON were upset about only getting $35 and two cartons of cigarettes. Victim 1 also stated that MILLER said he dropped DAWSON off and picked him up again after the robbery.

17. Based on my training and experience, I know most people commonly carry at least one mobile device with them when outside their residence. Whether actually on their person or close at hand, the vast majority of people keep their

mobile devices within close proximity wherever they go. This leads to a high probability that if law enforcement identifies the location of an individual's mobile device, the owner will be close by. I am also aware that violent crime conspiracies are often hatched in advance of the event, and often involve electronic communications between coconspirators and others before and after the crime is perpetrated. These communications often show planning and post-crime discussions, and are often conducted both in-person and utilizing messaging services on mobile devices. These communications often remain on providers' servers, on the involved mobile devices themselves, or both. Based on my training experience, I believe it is likely that, on the day of the robbery described above, MILLER was carrying the device associated with phone number 276-608-7196 and IMEI 352082504971013.

INFORMATION REGARDING WIRELESS PROVIDERS AND VERIZON

18. In my training and experience, I have learned that Verizon is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon subscribers may be located on the computers of Verizon. Further, I am aware that computers located at Verizon contain information and other stored electronic communications belonging to unrelated third parties.

19. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I understand that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Verizon for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

20. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long-distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

21. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identifier ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

22. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" and "faces" (i.e., antenna towers and specific directional antennae covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in

question. In addition to "tower and face" data, wireless providers sometimes store specialized location data about devices operating on their networks. Based on my training and experience, I know Verizon identifies this information as Enhanced 911 data and data recorded by their "Real Time Tool," also known as "Round Trip Tool" (RTT). RTT data can provide the location of a wireless device with greater precision than tower and face data alone, and can assist with determining what geographic vicinity a device was in at a particular time.

23. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

24. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand

the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Verizon to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Verizon. Because the warrant will be served on Verizon, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is

neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Special Agent Peter Gonzalves
Bureau of Alcohol, Tobacco, Firearms
and Explosives
United States Department of Justice

Subscribed and sworn to before me on July 28, 2021

HONORABLE PAMELA MEADE SARGENT
UNITED STATES MAGISTRATE JUDGE

Reviewed by: Whit Pierce, AUSA

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with (276) 608-7196 that is stored at premises owned, maintained, controlled, or operated by Verizon, a wireless provider whose Subpoena Compliance Department is headquartered at 180 Washington Valley Rd, Bedminster NJ 07921.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Verizon

To the extent that the information described in Attachment A is within the possession, custody, or control of Verizon, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Verizon or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Verizon is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from **May 1, 2021 through May 15, 2021**;

b. All text and multimedia messaging logs and content, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message from **May 1, 2021 through May 15, 2021**;

c. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device

associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

d. Detailed billing records, showing all billable calls including outgoing digits, from **May 1, 2021 through May 15, 2021**;

e. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from **May 1, 2021 through May 15, 2021**;

f. Incoming and outgoing telephone numbers (voice and SMS/MMS), including cell site and face data, from **May 1, 2021 through May 15, 2021**;

g. All specialized location data, including enhanced 911 data and RTT data from **May 1, 2021 through May 15, 2021**;

h. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

i. All records pertaining to communications between Verizon and any person regarding the account or identifier, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1951, Conspiracy to Interfere with Commerce by Threats or Violence (Hobbs Act Robbery) involving Michael MILLER and others on or about May 9, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence showing a conspiracy to commit robbery;

b. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

c. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

d. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s);

f. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the robbery, including records that help reveal their whereabouts.